

Claims:

1 A method of establishing a secure distributed system over a public network wherein
2 the system is a superstructure over the network, having a three-layer hierarchic
3 architecture comprising:

4 – a first layer having a *secure system authority*, which is a constant part in the secure
5 system;

6 – a second layer having a plurality of *secure servers*;

7 – a third layer having a plurality of *secure clients*, which are user nodes with installed
8 secure system client services;

9 wherein each secure server and each secure client may be incorporated into the
10 system at any time;

11 wherein the minimal number of secure clients in system is two and the minimal
12 number of secure servers is one;

13 wherein said secure servers, said secure clients and said secure system authority
14 are secure system nodes and provide a continuous secure sub-network over a public
15 network;

16 wherein any two secure system nodes, communicating via direct secure link within
17 the system, use a private ciphering language for encrypting and decrypting secure
18 message;

19 wherein each private ciphering language consists of two ciphering sets each
20 comprising a number (at least one) of ciphering algorithms and a collection of cipher-keys
21 for every algorithm;

22 wherein every ciphering set is used in one known direction of the secure link: one
23 ciphering set is used for encryption by the first link node and for decryption by the second
24 link node, and another ciphering set (in opposite direction) is used for encryption by the
25 second link node and for decryption by the first link node;

wherein a secure node registration with another secure node means that both nodes establish their private ciphering language for encrypting and decrypting a secure message transmitted between said secure nodes;

wherein every secure client can reach directly any secure server with which it is registered;

wherein every secure client can reach any other secure client via the mentioned above secure server(s);

wherein every secure server can reach another secure server directly within the system, or via other secure server(s), or via the secure system authority;

wherein every secure server is registered with the secure system authority;

wherein each secure client is registered with at least one secure server;

wherein two secure servers can be registered with one another;

wherein there is no other type of registration except for the mentioned above registration types;

wherein every secure message in addition to communication information according to the utilized communication protocol, contains specific secure communication information;

wherein the secure servers perform routing functions for a secure message as specified in the secure communication information;

wherein the secure system authority assists a secure server in determining a secure communication path, when required.

2 The method of establishing a secure distributed system of claim 1,

wherein any two *secure servers*, which do not have mutual ciphering language, can perform secure data transfer:

- either via the *secure system authority*,
- or using a one-time direct secure link with one another after secure connection is established between the *secure servers* by means of *secure system authority*.

1 3 The method of establishing a secure distributed system of claim 1,
2 wherein each cipher-key collection is unique - constructed specially for the
3 corresponding algorithm in current set;
4 wherein no cipher-key in said cipher-key collection is used more than once.

1 4 The method of establishing a secure distributed system of claim 3,
2 wherein after all keys in a cipher-key collection are used it is replaced by another
3 unique cipher-key collection;
4 wherein the key collection replacement can be performed either via the network
5 using current cipher-key collection, or by the cipher-key collection manual install.

1 5 The method of establishing a secure distributed system of claim 3, wherein the
2 message source node supplies to the message destination node corresponding index of the
3 cipher-key in the cipher-key collection for data decryption.

1 6 The method of establishing a secure distributed system of claim 1, wherein secure
2 multicast and broadcast transmissions are implemented by secure server(s) for
3 corresponding secure clients.

1 7 The method of establishing a secure distributed system of claim 1, wherein the end-to-
2 end secure communication information and the application data are always hidden
3 (ciphered).

1 8 The method of establishing a secure distributed system of claim 7, wherein the
2 application data and the secure communication information can be encrypted differently.

9 The method of establishing a secure distributed system of claim 8, wherein any secure
server can act during secure message transfer either as fully entrusted *secure server* -
Authorized Server, or as a mere secure router in secure system - Transit Server, according
to the message requirements.

10 The method of establishing a secure distributed system of claim 1,
wherein any message can be split into sub-messages;
wherein each sub-message is ciphered differently and transmitted as an
independent message via different *secure server* to a destination, where the sub -messages
will be assembled into a complete message;
wherein message split can be done either by the message source *secure client* or by
the *secure server*, appointed by the *secure client*;
wherein message assembling can be done either by the message destination *secure*
client or by the *secure server*, appointed by the *secure client*.

11 The method of establishing a secure distributed system of claim 4,
wherein any two *secure servers*, which are not registered with one another, can
perform secure data transfer:
- either via the *secure system authority*,
- or using a one-time direct secure link with another *secure server* after secure
connection is established by means of *secure system authority*.

12 The method of establishing a secure distributed system of claim 11, wherein the
message source node supplies to the message destination node corresponding index of the
cipher-key in the cipher-key collection for data decryption.

13 The method of establishing a secure distributed system of claim 12, wherein secure
multicast and broadcast transmissions are implemented by *secure server(s)* for
corresponding *secure clients*.

1 14 The method of establishing a secure distributed system of claim 13, wherein the end-
2 to-end secure communication information and the application data are always hidden
3 (ciphered).

1 15 The method of establishing a secure distributed system of claim 14, wherein the
2 application data and the hidden communication information can be encrypted differently.

1 16 The method of establishing a secure distributed system of claim 15, wherein any
2 *secure server* can act during secure message transfer either as fully entrusted *secure server*
3 - Authorized Server, or as a mere secure router in secure system - Transit Server,
4 according to the message requirements.

1 17 The method of establishing a secure distributed system of claim 16,
2 wherein any message can be split into sub-messages;
3 wherein each sub-message is ciphered differently and transmitted as an
4 independent message via different *secure server* to a destination, where the sub-messages
5 will be assembled into a complete message;
6 wherein message split can be done either by the message source *secure client* or by
7 the *secure server*, appointed by the *secure client*;
8 wherein message assembling can be done either by the message destination *secure*
9 *client* or by the *secure server*, appointed by the *secure client*.